ISMG Approved Meeting Minutes

Date: April 28, 2011
Time: 1:00 pm
Location: Walt Sullivan Building, First Floor conference room

Attendees

Pat Boles, SITSD; Michael Sweeney, DOA; Dan Delano, DOJ; Mike Jares, DEQ; Bill Hallinan, TRS; Kristi Antosh, MDT; Larry Krause, COM; Rick Bush, DNRC; Joan Anderson, OPI; Byron Molyneaux, OPI; Lance Wetzel, UID; Lynne Pizzini, SITSD; and Cindy Mitchell, SITSD.

Call to Order – Pat Boles

- Pat Boles called the April meeting to order.

Approval of Minutes – Pat Boles

- Pat asked for comments or changes to the March minutes. Kristi Antosh mentioned that the word "the" was inadvertently omitted from the last bullet on the 3rd page of the March minutes. Pat will make the change and have the minutes posted to the ITMC website.
  **** Action Item****
- Kristi Antosh motioned approval of the corrected minutes. Michael Sweeney seconded the motion.
  - Motion passed unanimously.

Approval of revised IS Access Control and IS Identification and Authentication Statewide Standards – Pat Boles

- Kristi submitted her changes to the document. Most of the changes involve using the word 'department' and 'agency' and more consistency across the two documents.
- Pat informed the group that DOA Legal Council has removed "Compliance" from Section V of the documents because these are standards not policies.
  ****Action Item****
- Kristi Antosh motioned for approval for Pat to make the necessary changes and submit for statewide review. Rick Bush seconded the motion.
  - Motion passed unanimously.

Approval for Information Security Programs Approach – Pat Boles

NIST 800-39 Managing Information Security Risk – Organization, Mission, and Information System View – Published March 2011

- Rick Bush asked Pat for clarification as to what is required for the July 1, 2012 deadline.
- Pat informed the group that that the proposed approach would have the following actions for each agency:
  - Develop the risk frame document
  - Document an initial assessment of your information systems
  - Modify the risk frame as needed based on the initial assessment by July 1, 2012.

- Rick Bush stated that he has no problem recommending that agencies have in place a "Risk Frame" but he has concerns about having an assessment completed by that time.
- The NIST 800-39 document specifies the information requirements required for the document. A template has not been found as of yet.
- The next part is taking the frame and initial assessment of the risks to identify what you are going to do going forward; this is where the planning and funding comes into play.
- Even though the frame and the initial assessment would be completed by July 1, 2012 this is a continuing process.
- Joan Anderson added that she believes she needs to understand the assessments for auditing purposes.
- Pat discussed that the Information Security Programs policy points to an out of date draft copy of NIST SP800-39. If the newly published SP800-39 (March 2011) is the document that the group would like to adopt, the policy needs to be updated to reflect this.

  ****Action Item****
- Rick Bush proposed the CIO office modify the policy to reflect the changes in the NIST 800-39 publication. Joan Anderson seconded the motion.
    - The motion passed unanimously.
- Lynne Pizzini informed the group that she created an assessment document for SABHRS and SITSD.
    - Lynne stated that she will share an assessment document that meets public transparency requirements.
    - An assessment must be completed for each system.
    - Categorization is determined through NIST. The controls associated will be identified through any SLA developed with the business user and SITSD.
    - Each NIST family must be refined within each assessment; it's not as cut and dried as one might think.
    - Templates would be nice to have so people don't confuse information systems with applications.
    - The first step is to identify the information system and then categorize it; which determines which controls are going to be applied to the information system and to any associated applications.
- Kristi Antosh informed the group that MDT is doing the initial assessments at a business function level and identifying what applications are utilized for each function. The executive management level will determine the most critical business functions. This will have an impact on the NIST requirements for the information system and associated applications.
- Pat informed the group that there will be more discussion on this topic at the next meeting.

Approval of ISMG Rules of Procedure – Pat Boles

****Action Item****

- Pat informed the group that he has modified the document and would like approval of the Operating Procedures.
- Lynne pointed out a correction on the 2nd page; change ITSD to SITSD.
    - Lynne also asked if the Information Security Officer should be added to the procedure. This will be done.
    - The ISSO will be provided by SITSD.
- Kristi Antosh moved approval of the ISMG Rules of Procedure with corrections provided by Lynne; motion seconded by Michael Sweeney.
    - The motion passed unanimously.

EPA ASSERT - Bill Hallinan

- Bill distributed a template of how he would like to engage and interact with the EPA Assert.
- Questions that came from the previous meeting demonstration are listed in the handout. This includes pricing of the components and Oracle DB hosting.
- The EPA Assert will help implement the NIST security controls.
- Bill said that it would be beneficial to talk to someone who actually works in the system instead of the program managers to receive 'real' feedback.
- Bill asked for group members to send him questions regarding the process.
- Rick Bush stated that he doesn't think this is a very expensive tool; but the question is who supports it?
- Bill stated that The Stanford Research Institute (SRI) put it together and he doesn't think that the hosting will be provided through EPA, but rather through SRI, if that is a possible option.
- Kristi said she doesn't think that we want to get ahead of ourselves by going to a tool without identifying the requirements.
- Bill stated that he is going to check with Chris from HHS and DOR for their opinion as to which type of configuration would be most appealing to them.
- Bill informed the group that he hears the consensus to follow-up on questions with the EPA, not for implementing purposes but for development guidance in the direction of going forward. He will have a report to distribute at the next meeting.
- The group unanimously agreed.
- Pat mentioned that he believes down the road that there are going to be other agency compliance requirements such as HIPAA, SOX, etc. While this may be a good tool for tracking against NIST, is it possible that it can assist in tracking compliance to the other mandates?

Other Business or Concerns – ISMG

- Pat mentioned there has been a change in the direction for the enterprise security function. With the departure from EISSB, it was determined that the bureau is no longer needed to meet the MITA requirements. It was determined that the security program function will be moving into the CIO Program Office. The ISSO function will continue to

be headed by Lynne. Pat expects that by the next meeting the vacancy announcement will have gone out.

- Kristi inquired about the MS-ISAC Training.
    - Lynne informed the group that she has previewed the training that has 19 modules; which take 3-10 minutes per module. One module is being developed for federal tax information. The online training with all modules is available for $1.15-$1.40 per seat depending on how many nationwide register for the program. Additional years will be cheaper as they will only pay annual maintenance. SITSD is in the process of purchasing the training for its staff as well as DOR. The cost is under $300.00 for SITSD.
    - Lynne needs to obtain a letter of intent from an authorized person at state agencies by June 15th. Payment must be made by July 31st.
    - The training has a tracking mechanism whereby agencies will be able to view reports for when individuals need to receive training updates. Agencies will also receive a validation when training is completed.
    - Lynne reported to the group that this MS-ISAC training meets the requirements needed for SITSD employees. This training will also meet the HIPAA requirement as well.
    - Lynne plans to inform her staff that they need to take two modules every month.
    - If we don't fill enough seats, the price will increase to around $1.40 per seat plus a maintenance fee that costs $0.58 cents for ongoing years. If you want to continue using for annual training, it will cost the $0.58 cents per user. MS-ISAC will send out an invoice to be paid from.
    - Lynne will forward more information on the MS-ISAC training as necessary.
- The agenda will be sent out one week prior to the next meeting and will be available through Sharepoint.

Adjourn – Pat Boles

- The meeting adjourned at 2:11 p.m.